APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,156	07/31/2003	Ronald P. Doyle	RSW920030063US1	1905

43168   7590   06/04/2007

MARCIA L. DOUBET LAW FIRM
PO BOX 422859
KISSIMMEE, FL 34742

EXAMINER
WYSZYNSKI, AUBREY H

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>15 March 2007</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,7,9,10,12,13 and 15-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,7,9,10,12,13 and 15-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>31 July 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1. The response of 3/15/07 was received and considered.

2. Claims 1, 4, 6-7, 15-17 and 19-20 have been amended.

3. Claims 1-4, 6-7, 9-10, 12-13 and 15-26 are pending.

Response to Arguments

4. Applicant's arguments with respect to claims 1-4, 6-7, 9-10, 12-13 and 15-26

have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 6-7, 9-10, 12-13 and 15-26 are rejected under 35 U.S.C. 102(e) as

being anticipated by Bourne et al, U.S. Patent Application Publication No.

2004/0168073.

Regarding Claim 1, Bourne discloses a security container (fig. 7, #310) that secures a

document component by encapsulating, within the security container, an encrypted

version of the document component, an encrypted version of conditional logic for

controlling operations on the document component, and key distribution information

usable for controlling access to the document component, wherein:

the encrypted version of the document component/content, and the encrypted version of

the conditional logic/rights data, are both encrypted using a first key/content key CK,

(fig. 7, #304 and #310);

the key distribution information comprises at least one key element; and each key

element comprises (i) an identification of a user, a user group, a process, or a process

group that is authorized to access the document component; and (ii) an encrypted

version of the first key, wherein the encrypted version of the first key/CK is encrypted

using a second key/Public key PU-DRM (fig. 7, "(PU-DRM(CK))") that is usable by the

identified user, user group, process, or process group for decrypting the encrypted

version of the first key, thereby enabling that user, user group, process, or process

group to obtain the first key and use it for decrypting the document component and the

conditional logic.

Regarding Claim 2, Bourne discloses the security container according to Claim 1,

wherein the security container secures a portion of a higher-level document/ signed

rights label SRL (fig. 7, #308).

Regarding Claim 3, Bourne discloses the security container according to Claim 2, wherein the higher-level document has more than one portion secured by security containers (fig. 4A).

Regarding Claim 4, Bourne discloses a method of securing document content using security containers/signed rights label SRL (fig. 4A, #308), comprising the step of encapsulating, within a security container, an encrypted version of a document component, an encrypted version of conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component, wherein:

the encrypted version of the document component/CONTENT INFO, and the encrypted version of the conditional logic/RIGHTSDATA, are both encrypted using a first key/K2 (fig. 4A);

the key distribution information comprises at least one key element; and each key element comprises (i) an identification of a user, a group of users, a process, a group of a processes that is authorized to access the document component; and (ii) an encrypted version of the first key/K2, wherein the encrypted version of the first key/K2, is encrypted using a second key/Public key PU-DRM (fig. 4A, "(PU-DRM(K2))") that is usable by the identified user, user group, process, or process group for decrypting the encrypted version of the first key, thereby enabling that user, group of users, process, or group. of processes to obtain the first key and use it for decrypting the document component and the conditional logic.

Regarding Claim 6, Bourne discloses the method according to Claim 4, wherein the first

key/K2, comprises a symmetric key/DES key (fig. 4, #408).

Regarding Claim 7, Bourne discloses the method according to Claim 6, wherein the

second key comprises, for each of the key elements, a public key associated with the

identified user, process, group of users, or group of processes (fig. 4, #414).

Regarding Claim 9, Bourne discloses the method according to Claim 4, wherein the

conditional logic further controls access to the document component (¶[0075]).

Regarding Claim 10, Bourne discloses the method according to Claim 9, wherein the

key distribution information further controls access to the conditional logic (¶[0075]).

Regarding Claim 12, Bourne discloses the method according to Claim 4, wherein the

security container is encoded in structured document format (¶[104]).

Regarding Claim 13, Bourne discloses the method according to Claim 12, wherein the

structured document format is Extensible Markup Language ("XML") format (¶[104]).

Regarding Claim 15, Bourne discloses the method according to Claim 4, wherein at

least one of the key elements identifies a group of users and wherein the users in the

group are determined dynamically, upon receiving a request to access to the document

component (fig. 6A, #606).

Regarding Claim 16, Bourne discloses the method according to Claim 15, wherein the

dynamic determination further comprises accessing a repository where the users in the

group are identified (fig. 6A, #610).

Regarding Claim 17, Bourne discloses the method according to Claim 4, further

comprising the steps of receiving, from a requester, a request to access the document

component; programmatically determining, using the key distribution information,

whether the requester is authorized to access the document component by determining

whether, in any selected one of the key elements, the requester is the identified user or

the identified process or is a member of the identified group of users or the identified

group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key

elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key, thereby

obtaining the conditional logic; decrypting the encrypted version of the document

component using the first key, thereby obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can be

granted; and, rejecting the request when the programmatically determining step has a

negative result (¶[0085] [0088] and fig 5).

Regarding Claim 18, Bourne discloses the method according to Claim 17, wherein the

conditional logic evaluates at least one of: an identity of the requester; a device used by

the requester; a context of the requester; a zone of an application used by the

requester; a user profile of the requester; and a target destination of the request

(¶[0089].

Regarding Claim 19, Bourne discloses a computer program product for securing

document content using security containers, the computer program product embodied

on one or more computer-readable media and comprising:

computer-readable program code for receiving, from a requester, a request to access

document content/content package (¶[0068], and fig. 11, #13), wherein the document

content is encapsulated as an encrypted version of a document component/(K2(CK))

(fig. 4, #408) within a security container/signed rights label SRL (fig. 4A, #308), along

with an encrypted version of conditional logic/rights data (K2(rightsdata)) (fig. 4, #416),

for controlling operations on the document component and key distribution information

usable for controlling access to the document component, wherein:

the encrypted version of the document component and the encrypted version of they

conditional logic are both encrypted using a first key/K2;

the key distribution information comprises at least one key element; and each key

element comprises (i) an identification of a user, a group of users, a process, or group

of a processes that is authorized to access the document component; and (ii) an

encrypted version of the first key/K2, wherein the encrypted version of the first key/K2 is

encrypted using a second key/public key PU-DRM (fig. 4, #404) that is usable by the

identified user, user group, process, or process group for decrypting the encrypted

version of the first key, thereby enabling that user, group of users, process, or groups of

processes to obtain the first key and use it for decrypting the document component and

the conditional logic;

computer-readable program code for programmatically determining, using the key

distribution information, whether the requester is authorized to access the document

component by determining whether, in any selected one of the key elements, the

requester is the identified user or the identified process or is a member of the identified

group of users or of the identified group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key

elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key, thereby

obtaining the conditional logic;

decrypting the encrypted version of the document component using the first key,

thereby obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can be

granted; and,

computer-readable program code for rejecting the request when operation of the

computer-readable program code for programmatically determining yields a negative

result (¶[0085] [0088] and fig 5).

Regarding Claim 20, Bourne discloses a system for securing document content using

security containers, comprising:

a security container/signed rights label SRL (fig. 4A, #308), that encapsulates an

encrypted version of a document component/content (fig. 4, #408), an encrypted

version of conditional logic/rights data (fig. 3, #416) for controlling operations on the

document component, an key distribution information (fig. 4, #420) usable for controlling

access to the document component, wherein:

the encrypted version of the document component and the encrypted version of the

conditional logic are both encrypted using a first key/K2;

the key distribution information comprises at least one key element; and each key

element comprises (i) an identification of a user, a group of users, a process, or group

of a processes that is authorized to access the document component; and (ii) a

encrypted version of the first key/K2, wherein the encrypted version of the first key/K2 is

encrypted using a second key/public key PU-DRM, that is usable by the identified user,

user group, process, or process group for decrypting the encrypted version of the first

key, thereby enabling that user, group of users, process, or groups of processes to

obtain the first key and use it for decrypting the document component and the

conditional logic;

means for receiving, from a requester, a request to access the document component;

means for programmatically determining, using the key distribution information, whether

the requester is authorized to access the document component by determining whether,

in any selected one of the key elements, the requester is the identified user or the

identified process or is a member of the identified group of users or of the identified

group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key

elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key, thereby

obtaining the conditional logic;

decrypting the encrypted version of the document component using the first key thereby

obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can be

granted; and,

means for rejecting the request when operation of the means for programmatically

determining yields a negative result (¶[0085] [0088] and fig 5).

Regarding Claim 21, Bourne discloses the system according to Claim 20, wherein the

security container is embedded within a document (¶[0084]).

Regarding Claim 22, Bourne discloses the system according to Claim 20, wherein the

security container encapsulates the document component on a system clipboard

(¶[0075]).

Regarding Claim 23, Bourne discloses the system according to Claim 20, wherein the

security container is place on a user interface (fig. 1, #160).

Regarding Claim 24, Bourne discloses the system according to Claim 20, wherein the

security container encapsulates the document component for exchange using

interprocess communications (¶[0051]).

Regarding Claim 25, Bourne discloses the system according to Claim 20, wherein the

security container encapsulates the document component for exchange using a

messaging system (¶[0051])

Regarding Claim 26, Bourne discloses the system according to Claim 20, further

comprising means for copying the document component to a target destination, wherein

the means for copying copies the entire security container in order to copy the

document component (¶[0076]).

Conclusion

7.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Aubrey H. Wyszynski whose telephone number is

(571)272-8155. The examiner can normally be reached on Monday - Thursday, and

alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER